



**7705 SAR-OS SAR-A/M Cryptographic  
Module (SARCM)**

**FIPS 140-2 Non-Proprietary Security  
Policy**

**FIPS Security Level:1**

Document Version: 1.2

November 19, 2018

## TABLE OF CONTENTS

<b>GLOSSARY .....</b>	<b>5</b>
<b>1. INTRODUCTION.....</b>	<b>7</b>
1.1 PURPOSE .....	7
1.2 VERSIONS AVAILABLE FOR FIPS.....	8
<b>2. SAR-OS CRYPTOGRAPHIC MODULE OVERVIEW.....</b>	<b>9</b>
2.1 SARCM CHARACTERISTICS.....	9
2.2 SARCM APPROVED ALGORITHMS .....	11
2.3 SARCM NON-APPROVED BUT ALLOWED ALGORITHMS .....	14
2.4 SARCM INTERFACES .....	14
<b>3. SARCM ROLES AND SERVICES.....</b>	<b>16</b>
<b>4. PHYSICAL SECURITY .....</b>	<b>18</b>
<b>5. OPERATIONAL ENVIRONMENT.....</b>	<b>19</b>
<b>6. KEY TABLE .....</b>	<b>20</b>
6.1 KEYS/CSPS ALGORITHMS IN FIPS-140-2 MODE .....	20
<b>7. EMC/EMI (FCC COMPLIANCE).....</b>	<b>23</b>
<b>8. SELF TESTS.....</b>	<b>24</b>
8.1 SELF TESTS ON THE CSM.....	24
8.1.1 <i>Cryptographic DRBG Startup Test</i> .....	25
8.1.2 <i>RSA Startup test</i> .....	25
8.2 CONDITIONAL TEST ON THE CSM .....	25
<b>9. FIPS-140 USER GUIDANCE .....</b>	<b>27</b>
9.1 FIPS-140-2 MODE CONFIGURATION.....	27

**7705 Series FIPS-140-2 Security Policy**

---

9.2 CONFIGURATIONS NOT ALLOWED WHEN RUNNING IN FIPS-140-2 MODE.....28

9.3 NON-FIPS-140-2 MODE.....29

10. REFERENCES.....31

**LIST OF FIGURES**

Figure 2-1: SARCM Diagram of Logical and Physical Boundaries.....9

**GLOSSARY**

<b>AES</b>	<i>Advanced Encryption Standard</i>
<b>BGP</b>	<i>Border Gateway Protocol</i>
<b>CBC</b>	<i>Cipher Block Chaining</i>
<b>CFM</b>	<i>Control / Forwarding Module</i>
<b>CLI</b>	<i>Command Line Interface</i>
<b>CMVP</b>	<i>Cryptographic Module Validation Program</i>
<b>CSM</b>	<i>Control Switch Module</i>
<b>CSP</b>	<i>Critical Security Parameter</i>
<b>CVL</b>	<i>Component Validation List</i>
<b>ESP</b>	<i>Encapsulating Security Payload</i>
<b>FIPS</b>	<i>Federal Information Processing Standard</i>
<b>GRE</b>	<i>Generic Routing Encapsulation</i>
<b>HMAC</b>	<i>Hashed Message Authentication Code</i>
<b>ICMP</b>	<i>Internet Control Message Protocol</i>
<b>ICV</b>	<i>Integrity Check Value</i>
<b>IGMP</b>	<i>Internet Group Management Protocol</i>
<b>IP</b>	<i>Internet Protocol</i>
<b>IPSec</b>	<i>IP Security</i>
<b>IS-IS</b>	<i>Intermediate System to Intermediate System</i>
<b>LDP</b>	<i>Label Distribution Protocol</i>
<b>LSP</b>	<i>Label Switched Path</i>

## 7705 Series FIPS-140-2 Security Policy

<b>MPLS</b>	<i>Multi-protocol label switching</i>
<b>NDRNG</b>	<i>Non-Deterministic RNG</i>
<b>NGE</b>	<i>Network Group Encryption</i>
<b>NIST</b>	<i>National Institute of Standards and Technology</i>
<b>OSPF</b>	<i>Open Shortest Path First</i>
<b>PFS</b>	<i>Perfect Forward Secrecy</i>
<b>RNG</b>	<i>Random Number Generator</i>
<b>RSVP</b>	<i>Resource Reservation Protocol</i>
<b>SA</b>	<i>Security Association</i>
<b>SAM</b>	<i>Service Aware Manager</i>
<b>SFM</b>	<i>Switch Fabric Module</i>
<b>SHA</b>	<i>Secure Hash Algorithm</i>
<b>SSH</b>	<i>Secure Shell</i>
<b>SPI</b>	<i>Security Parameter Index</i>
<b>TLS</b>	<i>Transport Layer Security</i>
<b>TM</b>	<i>Traffic Management</i>
<b>VPLS</b>	<i>Virtual Private LAN Service</i>

**Table 1 - Glossary**

## 1. INTRODUCTION

### 1.1 Purpose

This document describes the non-proprietary SAR-OS (Service Aggregation Router Operating System) Cryptographic Module (SARCM) Security Policy for the 7705 Service Aggregation Router (SAR) product family. These are referenced in the document as either 7705 or SAR.

This security policy provides the details for configuring and running the 7705 products in a FIPS-140-2 mode of operation and describes how the module meets the requirements of FIPS 140-2. Please see the references section for a full list of FIPS 140-2 requirements.

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1

11	Mitigation of Other Attacks	N/A
----	-----------------------------	-----

**Table 2 - Security Level per FIPS 140-2 Section**

## 1.2 Versions Available for FIPS

The following platforms of the 7705 products that implement the module are either tested or compatible for running SARCM in a FIPS approved mode:

Platform	Model(s)
7705 Service Aggregation Router (SAR) non-ipsec/ngc	SAR-A, SAR-M

**Table 3 - FIPS Capable Platforms and Models**

## 2. SAR-OS CRYPTOGRAPHIC MODULE OVERVIEW

The section provides an overview of the SAR-OS Cryptographic Module (SARCM) and the FIPS validated cryptographic algorithms used by services requiring those algorithms. The SARCM doesn't implement any services or protocols directly. Instead, it provides the cryptographic algorithm functions needed to allow SAR-OS to implement cryptography for those services and protocols that require it.

### 2.1 SARCM Characteristics

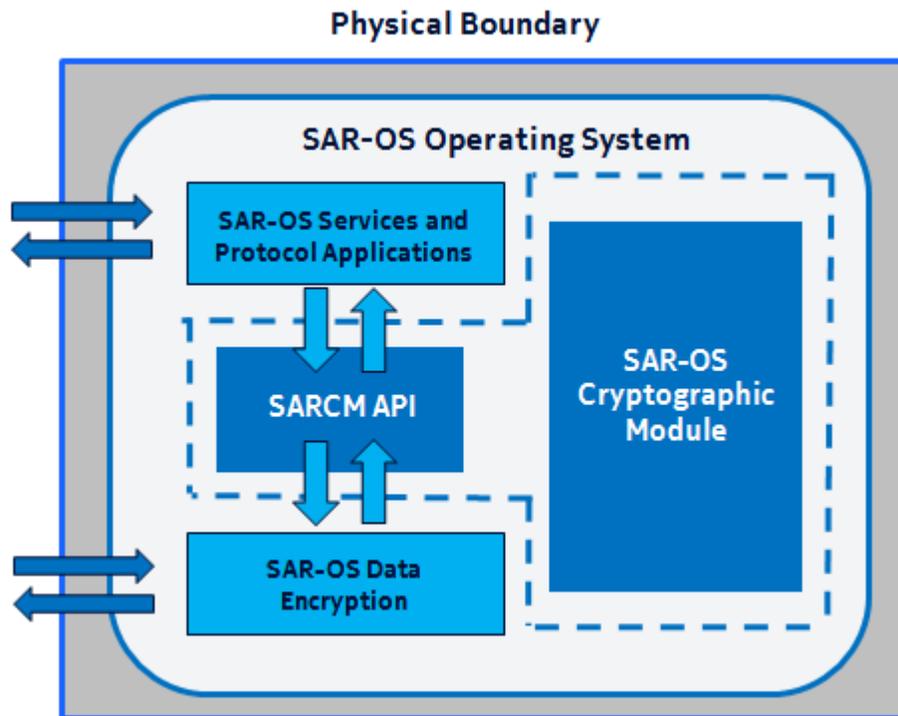


Figure 2-1: SARCM Diagram of Logical and Physical Boundaries

## 7705 Series FIPS-140-2 Security Policy

---

The SARCM logical and physical properties and boundary considerations is illustrated in Figure 2-1. The solid blue line represents the physical boundary of the cryptographic module that represents the hardware system on which SAR-OS is running and hence where SARCM is also running. The dashed blue line indicates the logical cryptographic boundary of the SARCM within SAR-OS. The SARCM is available as a cryptographic service for any SAR-OS services or protocols that require cryptographic operations.

The SARCM provides the cryptographic services required for the control plane (ie SNMPv3, routing protocols etc). On the 7705 SAR-A and SAR-M, all the control plane functionality is part of the Control and Switching Module (CSM), while the data plane is managed by the Winpath network processor. It should be noted on these platforms the CSM and line cards are physically on the same hardware, but logically separate. The winpath network processor on these platforms are not encryption capable. Per IG D.11, neither the CAVP nor the CMVP have reviewed or tested the SNMP protocol.

The SARCM is part of a single SAR-OS binary file (both.tim) that is used to run the full SAR-OS application. SARCM is classified as a multi-chip standalone software module and SARCM is included within the SAR-OS application code. SARCM has been validated on each CSM used by the hardware platforms listed in the following table. Note that the CSM is integrated into the chassis of 7705 SAR-M and A variants.

<b>Platform</b>	<b>Control Processor</b>
SAR-A	1 core @ 300 Mhz

## 7705 Series FIPS-140-2 Security Policy

	on chassis
SAR-M	1 core @ 500 Mhz on chassis

**Table 4 – Validated Hardware and FIPS Compatible Platforms**

The software version used to validate the SARCM was SAR-OS Rel 8.0R6.

### 2.2 SARCM Approved Algorithms

The SARCM uses the following FIPS approved algorithms:

CAVP CERT	Algorithm	Standard	Mode/M ethod	Key Lengths, Curves or Moduli	Use
4657	AES	FIPS 197, SP 800-38A	CBC	e/d, 128, 192, 256	Data encryption/decryption
4657	AES	FIPS 197, SP 800-38A	CFB	e/d, 128	Data encryption/decryption
4657	AES	SP 800-38B	CMAC	128	Message Authentication
-	CKG	SP 800-133	CKG	-	Cryptographic Key Generation

## 7705 Series FIPS-140-2 Security Policy

2478	Triple-DES <sup>1</sup> (TCBC)	SP 800-67	TCBC		Data encryption/decryption
2541	RSA	FIPS 186-4 SSA-PKCS#1- v1.5	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1024, 2048, 3072, 4096	Signature Verification
2541	RSA	FIPS 186-4		2048	Key Generation
2541	RSA	FIPS 186-4		2048	Signature Generation <sup>2</sup>
3085	HMAC	FIPS 198-1	HMAC-SHA1	112	Message Authentication
3085	HMAC	FIPS 198-1	HMAC-SHA-96	112	Message Authentication
3085	HMAC	FIPS 198-1	HMAC-SHA-224	224	Message Authentication
3085	HMAC	FIPS 198-1	HMAC-SHA-256, HMAC-	256, 384, 512	Message Authentication

<sup>1</sup> As of December 31<sup>st</sup>, 2015 two-key Triple-DES is Disallowed

<sup>2</sup> SHA-1 is not allowed for signature generation with RSA except for use within the TLS protocol

## 7705 Series FIPS-140-2 Security Policy

			SHA-384, HMAC- SHA-512		
1573	DRBG	SP 800-90A	AES-CTR	256	Derivation Function
1232	DSA	FIPS 186-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1024	Verification P&Q
1232	DSA	FIPS 186-4	SHA-224, SHA-256, SHA-384, SHA-512	2048	Key generation Verification P&Q
1232	DSA	FIPS 186-4	SHA-256, SHA-384, SHA-512	2048, 3072	PQG generation Signature generation Verification P&Q
1306	ASKDF, SSH	SP800-135	SHA1	SHA-1	

## 7705 Series FIPS-140-2 Security Policy

3816	SHA	FIPS 180-4	SHA-1, SHA- 224, SHA- 256, SHA- 224, SHA-512		
------	-----	------------	---	--	--

**Table 5 – Approved Algorithm Implementations**

There are algorithms, modes, and keys that have been CAVS tested but are not used by the module. Only the algorithms; modes and methods; key lengths, curves and moduli show in this table are used by the module.

### 2.3 SARCM non-Approved but Allowed Algorithms

The module supports the following non-FIPS approved algorithms which are:

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- NDRNG

### 2.4 SARCM Interfaces

The physical ports used by SARCM within SAR-OS are the same as those available on the system which is running SAR-OS per the platforms specified in the previous section. The logical interface is a C-language application program interface (API).

## 7705 Series FIPS-140-2 Security Policy

---

The Data Input interface consists of the input parameters of the API procedures and includes plaintext and/or cipher text data.

The Data Output interface consists of the output parameters of the API procedures and includes plaintext and/or cipher text data.

The Control Input interface consists of API functions that specify commands and control data used to control the operation of the module. The API may specify other functions or procedures as control input data.

The Status Output includes the return status, data and values associated with the status of the module.

The module provides logical interfaces to the other services within SAR-OS and those other SAR-OS services use the following logical interfaces for cryptographic functions: data input, data output, control input, and status output.

Interface	Description
Data Input	API input parameters including plaintext and/or cipher text data
Data Output	API output parameters including plaintext and/or cipher text data
Control Input	API procedure calls that may include other function calls as input, or input arguments that specify commands and control data used to control the operation of the module.
Status Output	API return code describing the status of SARCM

**Table 6 – FIPS 140-2 Logical Interface Mappings**

### 3. SARCM ROLES AND SERVICES

The SARCM meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing support for both the Crypto Officer and User roles within the SARCM. The support for both Crypto Officer and User roles within the SARCM is classed as a process. As allowed by FIPS 140-2, the SARCM does not support user authentication for these roles. Only one role may be using the SARCM at a time and the module does not allow concurrent operators to access the SARCM.

The User and Crypto Officer roles are implicitly assumed by the entity accessing the services implemented by the SARCM:

- Installation and initialization of the SARCM which is embedded in the SAR-OS image and installed on the SAR-OS platforms is assumed implicitly as the Crypto Officer when installation and initialization occurs.

The services available by the SARCM in FIPS mode to the Crypto Officer and User roles consist of the following:

Services	Access	Critical Security Parameters	Crypto Officer	User
Encryption	Execute	Symmetric keys AES, Triple-DES	X	X
Decryption	Execute	Symmetric keys AES, Triple-DES	X	X
Hash (HMAC)	Execute	HMAC SHA keys	X	X
Key generation	Write/execute	Symmetric key AES, Triple-DES, Asymmetric RSA, DSA, Diffie-Hellman public and private keys, HMAC key	X	X

## 7705 Series FIPS-140-2 Security Policy

Key agreement	Execute	DH public/private key	X	X
Perform Self-Tests	Execute/read	NA	X	X
DRBG	Read/Write/Execute	DRBG V, DRBG Entropy, DRBG Key	X	X
Show Status	Execute	NA	X	X
Signature signing	Execute	Asymmetric private key DSA, RSA	X	X
Signature verification	Execute	Asymmetric public key DSA, RSA	X	X
Zeroization	Write (zeroize)	Symmetric key, asymmetric key, HMAC-SHA keys, seed key, seed	X	X
Module Initialization	Execute	All CSPs	X	
Routing (OSPF, IS-IS, RSVP)	Execute	HMAC SHA keys	X	X

**Table 7 – Module Services**

#### 4. PHYSICAL SECURITY

The module obtains its physical security from any platform running SAR-OS with production grade components and standard passivation as allowed by FIPS 140-2 level 1.

**5. OPERATIONAL ENVIRONMENT**

The SARCM was tested on the following platforms that represent the required HW components that runs SAR-OS and the SARCM.

<b>Platform used for testing/validation</b>	<b>Hardware running SAR-OS</b>
SAR-A	1 core Cavium Octeon Plus @ 300 Mhz on chassis
SAR-M	1 core Cavium Octeon Plus @ 500 Mhz on Chassis

**Table 8 – Hardware and Platforms Used to Test Module**

## 6. KEY TABLE

### 6.1 Keys/CSPs Algorithms In FIPS-140-2 Mode

The following keys and CSPs are available when running in FIPS-140-2 mode for the SARCM:

Key or CSP	Usage (Service)	Storage	Generation/Input	Zeroization	Access Role (R,W,X)
Triple DES-CBC	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-128-CFB	SNMPv3	Non-Volatile memory	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-128-CBC	SSHv2, Secure Copy, SFTP	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-192-CBC	SSHv2, Secure Copy, SFTP	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-256-CBC	SSHv2, Secure Copy	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
AES-128-CMAC	Message Authentication	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
HMAC-SHA-1	OSPF, IS-IS, RSVP, Software	DRAM (plaintext)	Operator – Manually	Command	R, W

## 7705 Series FIPS-140-2 Security Policy

	Integrity				
HMAC-SHA-1	SSHv2,	DRAM (plaintext)	Operator – Manually	Command	R, W, X
HMAC-SHA-256	OSPF, IS-IS, RSVP	DRAM (plaintext)	Operator – Manually	Command	R, W
HMAC-SHA-1-96	SNMP, SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
DSA Public Key 1K, 2K, 3K	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
DSA Private Key 2K, 3K	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
RSA Public Key 1K, 2K, 4K	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
RSA Private Key 2K, 4K	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
Diffie-Hellman Public Key Group 14 (2048- bit)	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
Diffie-Hellman Private Key Group 14 (2048- bit)	SSHv2	DRAM (plaintext)	Approved DRBG, API parameter	Reboot, Command	R, W, X
DRBG Seed	Key generation	DRAM (plaintext)	Internally Generated	Reboot	R, W
DRBG Entropy	Key generation	DRAM (plaintext)	Internally Generated	Reboot	R, W

## 7705 Series FIPS-140-2 Security Policy

DRBG 'V' Value	Key generation	DRAM (plaintext)	Internally Generated	Reboot	R, W
DRBG 'Key' Value	Key generation	DRAM (plaintext)	Internally Generated	Reboot	R, W

**Table 9 – Cryptographic Keys and CSPs**

Access roles include "R"- Read, "W" – Write, and "X" – Execute.

No parts of the SSH protocol, other than the KDF, have been tested by the CAVP.

The user is responsible for ensuring the module is limited to  $2^{16}$  encryptions with the same Triple-DES key. The module implements SP 800-90A compliant DRBG services for creation of symmetric keys, and for generation of DSA and RSA keys as shown in Tables 5 and 9. Resulting symmetric keys are an unmodified output from an Approved DRBG.

The estimated amount of entropy provided by the NDRNG is 0.22 per 1 bit of data. The DRBG accepts 2048 bits of data from the NDRNG as a seed.

## 7. EMC/EMI (FCC COMPLIANCE)

The SAR chassis where the CSM, SAR-OS and SARCM runs were tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

## **8. SELF TESTS**

### **8.1 Self Tests on the CSM**

When FIPS-140-2 mode is enabled the node performs the following startup tests:

- Software integrity check on startup using HMAC-SHA-1<sup>3</sup>
- Triple-DES encrypt KAT
- Triple-DES decrypt KAT
- AES encrypt 128, 192,256 KAT
- AES decrypt 128, 192,256 KAT
- HMAC SHA-1 KAT, HMAC SHA-224 KAT, HMAC-SHA-256 KAT, HMAC SHA-384 KAT, HMAC SHA-512 KAT
- SHA-1 KAT, SHA-224 KAT, SHA-256 KAT, SHA-384 KAT, SHA-512 KAT
- RSA sign and verify
- DSA sign and verify

Should any of these tests fail, the SARCM does not allow the node to continue booting the image. An error is displayed on the console port that indicates the failed test and the SARCM forces a reboot to attempt the self-tests again.

---

<sup>3</sup> The HMAC key size used is 128 bits

### **8.1.1 Cryptographic DRBG Startup Test**

A known answer test is used by the DRBG on startup (by using a known seed). If the startup test fails then an error message is printed on the console and the node will attempt the boot sequence again.

### **8.1.2 RSA Startup test**

SARCM performs an initial startup test with a known public key, a known digital signature and a test that verifies it can perform a proper verification of the known signature with the known public key. If the SARCM fails to successfully perform this startup test, then a message is printed on the console, the SARCM causes the node to reboot and tries to perform all the startup tests successfully again from the beginning.

## **8.2 Conditional Test on the CSM**

When FIPS-140-2 mode is enabled the node performs the following conditional self tests during normal operation of the node:

- Manual Key Entry Tests
- Pairwise Consistency Test for RSA / DSA
- SP800-90A DRBG Continuous Random Number Generator Test (CRNGT)
- NDRNG Continuous Random Number Generator Test (CRNGT)

Descriptions of the tests are described in the following sections.

### **SARCM Failure**

## 7705 Series FIPS-140-2 Security Policy

---

When a Conditional Test (e.g. the pairwise consistency tests or the CRNGT test) fails, then the SARCM is considered as failed. The node will print a message on the console that indicates that the SARCM has failed.

### 9. FIPS-140 USER GUIDANCE

The following sections described the SAR-OS user guidance for configuring the SAR systems where the SARCM is embedded and accessed by SAR-OS.

#### 9.1 FIPS-140-2 Mode Configuration

To enable FIPS-140-2 on the 7705 a configurable parameter is available in the bof.cfg file. The command “/bof fips-140-2” needs to be typed in and followed by a “/bof save” and reboot of the node. When configured in the bof.cfg, the node boots in FIPS-140-2 mode and the following behaviors are enabled on the node:

- Only FIPS-140-2 approved algorithms (except for two-key Triple-DES and Diffie-Hellman with key sizes less than 2048 bits) are available for encryption and authentication for any cryptographic function on the CSM where SAR-OS and the SARCM reside
- Two-key Triple-DES and Diffie-Hellman with non-compliant key sizes must not be used in FIPS mode; otherwise the module will enter a non-FIPS mode.
- Startup tests are executed on the CSM when the node boots
- Conditional tests are executed when required during normal operation (e.g. manual key entry test, pairwise consistency checks and RNG tests)

The current state of the bof and the parameters used for booting can be verified with the following CLI commands:

```
*A:bkvm12>show bof
```

```
*A:bkvm12>show bof booted
```

## 7705 Series FIPS-140-2 Security Policy

---

Output of the command “show bof booted” will show a line entry “fips-140-2” to indicate the module is now operating in FIPS Approved mode.

Note the FIPS-140-2 parameter in the bof.cfg does not take effect until the node has been rebooted. When running in FIPS mode the system will display a value in the system command that indicates this is the case.

### 9.2 Configurations Not Allowed when running in FIPS-140-2 Mode

When the node is configured in FIPS-140-2 mode the following disallowed algorithms are visible in CLI but not available. The User must not configure the following algorithms and functions when running in FIPS-140-2 mode or reverse the configuration steps in Section 9.1:

- MD5
  - SNMP, OSPF, BGP, LDP, NTP authentication, multi-chassis redundancy
- HMAC-MD5
  - SNMP, IS-IS, RSVP
- HMAC-MD5-96
  - SNMP
- HMAC-SHA-1-96
  - OSPF, BGP, LDP
- AES-128-CMAC-96
  - BGP, LDP

### 9.3 Non-FIPS-140-2 Mode

During operation, the module can switch modes on a service-by-service basis between an Approved mode of operation and a non-Approved mode of operation. The module will transition to the non-Approved mode of operation when the “Key agreement” service is invoked using non-compliant Diffie-Hellman key sizes (less than 2048 bits). This includes key sizes of 512 and 1024 bits. The module will also transition to the non-Approved mode of operation when the “Encryption” service is invoked using Two-key Triple DES. The module transitions back to the Approved mode of operation upon the utilization of an Approved security function.

The module supports the Crypto Officer and User roles while in the non-Approved mode of operation.

Table 10 below lists the service(s) available in the non-Approved mode of operation.

Services	Access	Critical Security Parameters	Crypto Officer	User
Encryption (non-compliant when using Two-key Triple DES)	Execute	Triple-DES	X	X
Key agreement (non-compliant)	Execute	DH public/private key	X	X
Keyed Hash	Execute	HMAC-ripemd160 key	x	x

## 7705 Series FIPS-140-2 Security Policy

(HMAC-ripemd160)				
Keyed Hash (HMAC-ripemd160@openssh.com)	Execute	HMAC-ripemd160 key@openssh.com	x	x

**Table 10 – Non-Approved Services**

### 10. REFERENCES

- [FIPS 140-2] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001, CHANGE NOTICES (12-03-2002).  
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- [FIPS 140-2 DTR] Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, January 4, 2011 Draft.  
<http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402DTR.pdf>
- [FIPS 140-2 IG] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, May 25, 2018.  
<http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf>